Scenario: Influences to EU civil security emanating from conflict zones

The fifth annual report in EXERTER

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 786805

EXERTER
Scenario: Influences to EU civil security
emanating from conflict zones -
The fifth annual report in EXERTER

FOI-2017-1045
April, 2023

Photo: FOI

EXERTER

Security of Explosives pan-European Specialists Network

The EXERTER network is a European initiative that seeks to identify and promote innovative methods, technologies, and tools to combat terrorism and serious crime, thereby improving the Security of Explosives. The network brings together a team of experts from Law Enforcement Agencies (LEAs), military institutes, governmental and civilian research institutes, academia, and standardisation organisations.

By fostering the exchange of information on current and emerging threats, operational requirements, and the state of research and innovation, EXERTER empowers practitioners with the knowledge and tools they need to enhance the security of our society. Each year, the network focuses on a series of scenarios related to the Security of Explosives, aiming to identify weaknesses in our response and opportunities for improvement. EXERTER focuses on standardisation, certification, research, innovation, and exploitation.

In its fifth year, the scenarios explored by EXERTER concern influences to EU civil security emanating from conflict zones. This report summarises the network's findings, analyses, and recommendations based on this year's scenarios.

Introduction

EXERTER focuses each year on a specific scenario or set of scenarios identified with input from practitioners and experts. The network then addresses related issues in all four phases of the timeline: PREVENT, DETECT, MITIGATE, and REACT. It examines the requirements, gaps, research, standardisation, and certification activities and strives to implement innovations in all phases.

The countermeasures for each domain differ technically and operationally and target different users and stakeholders, setting a broad scope for EXERTER. This report summarises the results of EXERTER's work on scenarios involving influences to EU civil security emanating from conflict zones. It provides an overview of the findings in each counter-attack domain and presents conclusions and recommendations for future directions and needs.

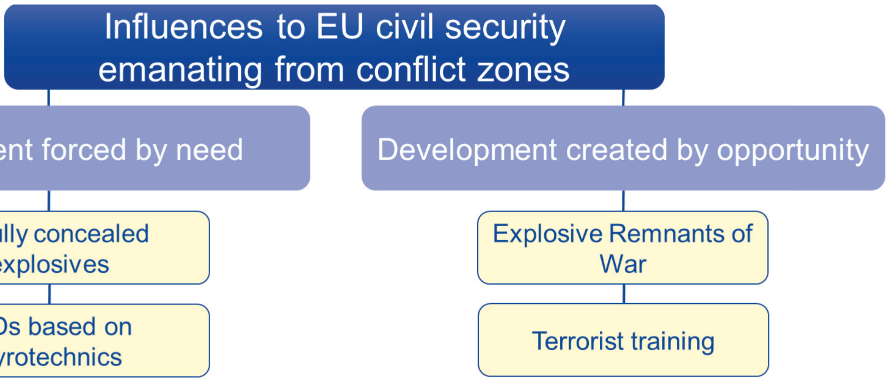
At the start of EXERTER's yearly cycle, the practitioners' requirements and gaps for countering the threat scenario were identified. These were based on analysing input from stakeholders and the expert community. The information was collected in a classified report and was the foundation for the network's continued work.

PREVENT...
DETECT...
MITIGATE...
REACT...
...preparation & production
...transportation
...attack
...post attack
ALERT

Scenarios

Influences to EU civil security emanating from conflict zones

Events in conflict zones drive new ways to create improvised attacks, and related information transpires outside the conflict zone. That has been historically observed and is likely to continue to influence future modi operandi in Europe. Here, we focus on four subtopics.


Influences to EU civil security emanating from conflict zones
Development forced by need
Development created by opportunity
Artfully concealed explosives
IEDs based on Pyrotechnics
Explosive Remnants of War
Terrorist training

Artfully concealed explosives: Our adversaries must get explosives through customs or security checkpoints to perform an attack. Cases of artfully concealed explosives include the shoe bomber, liquid explosives in unopened drink bottles, the underwear bomber, and the printer cartridge bomb plot. Further possibilities include coloured, moulded, or printed explosives, hidden in objects or containers or mixed with other substances to evade detection. At the same time, techniques for smuggling drugs can be applied to explosives smuggling.

IED based on pyrotechnics: This subtopic concerns using pyrotechnics based on need due to lacking access to more powerful explosives or simply earlier success with pyrotechnics. An example of transfer of the use of pyrotechnics is the IED construction used in the attack on Boston Marathon in 2013.

Explosive remnants of war: Post-conflict environments are exploited to support criminal and terrorism-related activities. Many European countries still have unexploded ordnance and other remnants of World War II that were dumped on land, in lakes, and even in the maritime environment. These explosives have not degraded and remain easily accessible for illicit use. The war in ex-Yugoslavia continues to supply criminals with weapons and explosives, and a similar situation may arise following the conclusion of the Ukraine war.

Terrorist training: Europol's "EU Terrorism Situation and Trend Report" states that the threat of terrorism to the EU remains high. Several individuals were arrested in 2021 after they had received terrorist training in conflict zones. Extremist organisations also provide online training and encourage individuals to attack their homeland. More online activity and isolation during the covid-19 pandemic have increased the risk of radicalising vulnerable individuals. Additionally, suspected terrorists are being trained to produce and use a new explosive material not included in standard detection instruments.

Prevent

The Prevent domain in Year 5 addresses the risks associated with artfully concealed explosives, IEDs based on pyrotechnics, explosive remnants of war, and terrorist training. The chapter highlights initiatives and strategies for restricting access to materials and knowledge and strengthening international cooperation and information sharing. It also emphasises the need to monitor and regulate the online space, where radicalisation and training often occur. Public-private partnerships and community engagement are crucial to identify and prevent potential threats before they materialise.

Research initiatives and collaboration

Several projects have addressed security challenges, including preventing concealed explosives, smuggling explosive remnants of war. The challenge to preventing the smuggling of explosive remnants of war (ERWs) lies in the inherent difficulty of detecting and intercepting these dangerous materials. Smugglers often use complex and innovative methods to conceal ERWs, making their detection challenging for security forces. Moreover, the vastness of international borders and the high volume of trade and travel increase the difficulty of thoroughly monitoring and inspecting all cargo and travellers.

The UNCOVER project seeks to enhance intelligence work to uncover attack plans involving concealed explosives. ANITA, ENTRANCE, and PARSEC focus on preventing the smuggling of explosives and improving checkpoint security.

Photo: FOI

PARSEC, in particular, aims to develop new technologies to detect illegal parcels in postal services.

The challenges of countering radicalisation and improving checkpoint security involve addressing complex factors and balancing effective prevention measures with minimal disruptions. Radicalisation prevention requires understanding of its root causes, identifying at-risk individuals, and combating the spread of extremist content online. That necessitates collaboration between governments, technology companies, and civil society organisations. The following projects have focused on the topic of radicalization and improving checkpoint security.

To prevent radicalization, the PROHETS and CounteR projects have developed toolkits and platforms for reducing the number of individuals trained as terrorists. LAW-GAME uses gamification technologies to train police officers on effective experiential training and prediction of criminal actions.

UNCOVER also works on developing an efficient steganalysis framework to detect hidden information in digital media. ANITA targets online illegal trafficking by creating a user-centred investigation system. ENTRANCE aims to improve the non-intrusive inspection of cross-border freight movements through risk-based approaches. PARSEC focuses on parcel and letter security for postal and express courier flows by developing non-intrusive detection technologies.

Prohets and counter both aim to prevent future terrorist attacks by developing eu-wide security models and privacy-first situational awareness platforms, respectively, for data mining and prediction of critical areas.

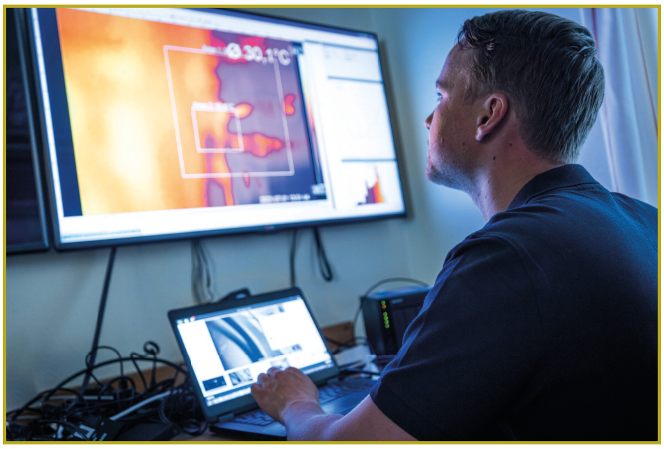


Photo: FOI

Examples of possible future initiatives:

- Limiting access to precursor materials for 3D printing IEDs and considering the need to register purchases of 3D printers.
- Collaboration with counter-narcotic forces to exchange experiences and applied methods.
- Financial support to incentivise people to hand in explosive remnants of war.
- Surveillance of foreign territory fighters and training camps to prevent terrorist activity.

Detect

Detection efforts focus on identifying concealed explosives, pyrotechnic-based IEDs, remnants of war, and individuals who have received terrorist training. The chapter emphasises developing and implementing advanced detection technologies and methodologies to identify various threats accurately. These include sensors and systems capable of detecting concealed and disguised explosives and monitoring and analysing online activity to identify potential terrorist training or radicalisation. Cross-border collaboration, data sharing, and integrating detection technologies within the security infrastructure are crucial for effective threat detection.

Research Initiatives

Not all detection technologies are equally suited for all scenarios; some require training, well-developed and exercised SOPs, and mechanical and logistic support. For some of the selected scenarios, cost-effective measures can be widely and easily implemented.

At European level, there are several research initiatives where the developed tools could potentially be applied; for example, MiRTLE is a low-cost threat detection system by Radio Physics Solutions that can detect concealed weapons and explosives up to fifty metres away. CONSORTIS aims to develop a stand-off concealed object detection demonstrator using a dual-frequency submillimetre-wave video camera and active 3D imaging radar system. TERASCREEN seeks to create a security screening technology for border checks using passive and active operation at several Terahertz frequencies. VMEWI3 aims to develop a technology demonstrator using remotely operated unmanned ground vehicles to detect indirect indicators of IED presence. MUSICODE will develop new unmanned ground vehicle stand-off capabilities to detect IED components. CONFIDENT aims to develop technology demonstrators using remotely operated platforms to confirm and identify IED components and provide complementary early warning capability. MKD proposes a new system of landmine detection based on unmanned aerial vehicles. COSMIC proposes a three-stage detection system with eight CBRNE sensors to detect CBRNE materials hidden in shipping containers and vehicles.

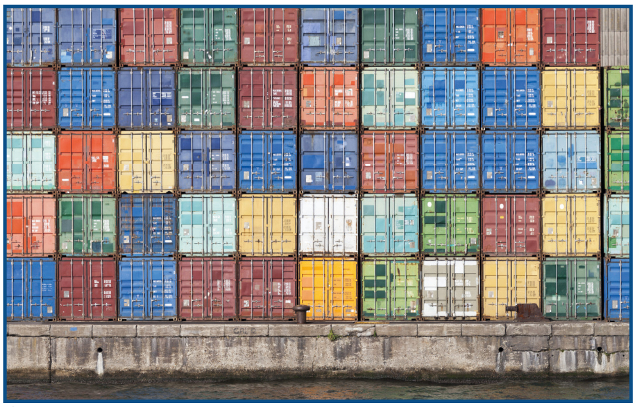


Photo: FOI

Exploration and development of new technology

A crucial factor for new detection technology is its ability to adapt to ever-changing attack methods rapidly. Suggested actions include standardised validation for their intended use, assessing cost-effectiveness, establishing EU-wide standardisation to address user needs better, and facilitating shared access to data sets at the EU level.

Collaboration

Successful innovation in the security industry relies on more than government initiatives like public funding or legislation. A promising future necessitates active involvement, commitment, and partnership from potential clients in the security sector, as well as proactive collaboration between various stakeholders, such as governments, regulators, policymakers, industry, innovators, research teams, and users. This collaboration accelerates innovation and ensures the efficient integration of innovative solutions into the security landscape.

Technologies suggested for further development:

- Continuous technology updates and personnel education to detect emerging threats is needed.
- Concepts to detect pyrotechnic materials and bomb-making factories are essential.
- Improved intelligence and detection methods to disrupt smuggling activities should be applied.
- Biometric identification and centralised databases to spot suspicious individuals and patterns are considered valuable.

Mitigate

In the described circumstances, the possibilities to mitigate the effect of explosives are independent of the underlying motivation of a perpetrator. Here, we highlight the importance of protecting existing infrastructure and striving for it during planning and construction. Quantitative risk analysis is one tool that can guide the decision process by balancing costs and effectiveness.

Research areas

Structural and design measures that mitigate explosion effects are available and have been investigated in various research projects. The specific applicability of each action depends on the location of interest, and a cost-benefit analysis should be conducted. During the design phase of places or buildings, fundamental mitigation aspects, such as safeguarding the distance between the target and potential attack, can be considered. Hazards from fragmentation can be reduced using blast-resistant components and appropriate separation of places. Organisational measures that can minimise explosion effects include reducing people's exposure, evacuating people, and training first responders. First responders do not know what kind of explosive might be inside the IED. Instead, the response to an attack depends on the location and surroundings of the IED.

Research initiatives

Physical and organisational mitigation measures for EU civil security depend on the location and surroundings of IEDs rather than the type of IED. Research projects such as AURIS, ELASSTIC, SPIRIT, SUSQRA, and TACTICS have developed tools, technologies, and methods to enhance security, reduce damage, and improve attack response. AURIS established a security management system for critical infrastructure and building health monitoring. ELASSTIC focused on building design and sensor technology. SPIRIT developed tools to enhance the security of large buildings against terrorist threats.

Photo: FOI

SUSQRA aimed to create software for post-blast IED damage evaluation. TACTICS developed tools for improving security forces' ability to prevent and handle urban attacks.

Further Research

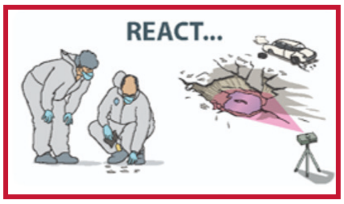
Consequently, a field for further research could be identifying simple and cheap technological and organisational measures to mitigate explosion effects, whenever this always has to go hand in hand with the prevent- and detect measures. The basis could be quantitative risk analysis, where different kinds of measures, their costs, and their effectivity are evaluated against each other.

Photo: FOI

Suggested measures include:

- Infrastructure known as a target for attacks can be put where their destruction limits collateral damage.
- Organisational measures that can minimise explosion effects include reducing people's exposure, evacuating people, and training first responders.
- Making existing solutions available and research results easily accessible to end users

React



The React domain in Year 5 focuses on emergency management and response in the context of concealed explosives, pyrotechnic-based IEDs, explosive remnants of war, and terrorist training. The chapter discusses the importance of swift and effective incident response, including interagency coordination and communication. It also emphasises the need for advanced training and resources for first responders, law enforcement, and medical personnel to minimise casualties and ensure the safety of affected individuals. Lastly, the chapter highlights the significance of post-incident investigations, analysis, and information sharing to improve future prevention, detection, and mitigation efforts.

To REACT to the terrorist attack timeline requires improved collaboration and communication between European forensic and research institutes and first responders, police, law enforcement, and the judiciary. Projects such as ACRIMAS, AUGGMED, CAST, XClanLab, RISEN, ROSFEN, BRIDGE, DARIUS, DirtyBomb, GIFT-CBRN, and PRACTICE aim to facilitate this cooperation by providing training for coordinated and rapid response to attack scenarios, enabling first responders to assess a crisis without endangering themselves, developing solutions for stable and uniform crisis management, and exchanging expertise regarding new solutions necessary to civil security. These projects also prepare for realistic threats, for example, dirty bombs, attacks on critical infrastructure, and remote-operated vehicle attacks.

Challenges & possibilities in React

There are still many challenges to overcome with respect to combating and reacting to the chosen scenarios. Improved and more extensive monitoring and surveillance of the trafficking of illicit material on the darknet, could reduce the number of attacks. In addition, the surveillance of social media could be intensified.

Photo: FOI

Research on organizational measures is suggested regarding:

- Improvement of post-blast investigation concerning forensics, but also information sharing are suggested.
- Combination of efforts is likely beneficial to follow and anticipate developments in the scene.
- Tracing the origin of used explosives and other components.
- EODs should prepare for emerging threats, and publishing HME synthesis should be limited in scientific literature.

Forensic investigation. Photo: FOI

Surveillance of social media. Photo: FOI

Concluding remarks

Our research has identified a range of innovative technologies, procedures, and strategies that hold the potential to enhance public safety across the four counter-attack domains significantly: Prevent, Detect, Mitigate, and React. We rigorously evaluated these options in light of the annual scenarios considered.

In the Prevent domain, initiatives aim to identify and track potential threats. In contrast, the Detect domain highlighted advances in surveillance and stand-off detection techniques. The Mitigate domain focused on addressing challenges in soft targets and infrastructure protection. The React domain emphasised the importance of forensic analysis and improved communication between actors.

It is essential to consider the context of any project deployment and the potential consequences on individual freedom, higher costs, and societal disruption. Striking the right balance between security and potential negative societal impacts is crucial. Proposed solutions must be assessed for their effects on individual rights and freedoms, as well as their financial viability and sustainability.

In conclusion, our study has revealed significant findings with the potential to contribute to developing more effective public safety strategies across the four counter-attack domains. Policymakers and practitioners must acknowledge that these initiatives require careful evaluation and tailoring to meet community needs and conditions. We hope our work will be a foundation for further research and discussion in this critical area.

Please visit our EXERTER's web-page, or contact us for more information about our work and activities.

EXERTER consortium

FOI
FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment
Fraunhofer EMI
Fraunhofer ICT
ENEA
TNO innovation for life
Polisen
KEMEA
INTERPOL
Bundeskriminalamt
WAT
KOMENDA STOŁECZNA POLICJI
POLICJA WARSZAWA
POLICIJA
RH MUP
INTA
RGNF
DEC C-IED
POLICE SERVICE NORTHERN IRELAND
Keeping People Safe